



# Extreme Networks Solutions Selling: ExtremeManagement Knowledge Transfer

**Abstract:** This document has been created for the use of Extreme Networks SEs and Partners. The primary purpose of this document is to serve as textbook style training material used in conjunction with the ExtremeManagement 200 level training course. The content in this particular document focuses on the transfer of technical knowledge necessary to provide Extreme SEs and partners foundational knowledge supporting the technical skillsets required to design an ExtremeManagement system.

**Published:** February 2018

Extreme Networks, Inc.  
145 Rio Robles  
San Jose, California 95134  
Phone / +1 408.579.2800  
Toll-free / +1 888.257.3000  
[www.extremenetworks.com](http://www.extremenetworks.com)

© 2012–2018 Extreme Networks, Inc. All Rights Reserved.

AccessAdapt, Alpine, Altitude, BlackDiamond, Direct Attach, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodriven, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Ridgeline, SentiAnt, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, XNV, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodriven logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is the property of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

For additional information on Extreme Networks trademarks, see

[www.extremenetworks.com/company/legal/trademarks](http://www.extremenetworks.com/company/legal/trademarks).

# Contents

---

<b>PaloAlto integration .....</b>	<b>4</b>
<b>Why = Use Cases. ....</b>	<b>4</b>
<b>Extreme Policy vs. Firewall .....</b>	<b>4</b>
<b>How it works – XMC -&gt; PaloAlto .....</b>	<b>5</b>
<b>LDAP - &gt; Extreme Control -&gt; Policy -&gt; XMC -&gt; PaloAlto.....</b>	<b>6</b>
<b>How Distributed IPS (DIPS) works – PaloAlto -&gt; XMC .....</b>	<b>10</b>
<b>DIPS: PaloAlto -&gt; XMC .....</b>	<b>10</b>
<b>Configuration options XMC .....</b>	<b>13</b>
SNMP configuration (not necessary for User-ID mapping):.....	13
Connect configuration: .....	14
DIPS configuration:.....	15
<b>Configuration options PaloAlto .....</b>	<b>16</b>
SNMP configuration (not necessary for User-ID mapping):.....	16
LLDP configuration (not necessary for User-ID mapping): .....	17
API role (for User-ID integration):.....	18
API user (for User-ID integration):.....	19
DIPS configuration:.....	20
<b>Terms &amp; Condition of Use.....</b>	<b>22</b>
<b>Revision History .....</b>	<b>23</b>

## PaloAlto integration

---

With Extreme Control the customer does have visibility of each end-system attached to the network = Username, IP, location, ... The Firewall is very limited getting information about user location, username, end-system device. We can provide mapping of username-IP to the firewall. Firewall can apply different approach to traffic generated by that IP.

Next Generation firewall can get information about username by:

- Reading Active Directory logs = not every device is in AD (not only managers are happy with Mac)
- Getting the Kerberos protocol information (logging to AD) = kerberos authentication does generate ticket to the user. The ticket is valid for specific time period. If the user moves from wired to wireless or from one zone to other and get new IP address the new ticket is not generated => firewall does not get this information
- Getting the information from the end-system = not every end-system can be reconfigured to support it. Sometimes the way is only through web browser, but not every user does use web browser every time...

Next Generation firewall can block the traffic if the traffic is processed by the firewall only. Firewall cannot block horizontal communication = communication within the subnet not passing the firewall.

### Why = Use Cases.

Customer can apply different Firewall Rules, AntiVirus settings, URL filtering, AntiSpyware, File Blocking, Data Filtering, ... based on user group. = Different firewall rules for sales team comparing to engineering team, different URL filters for different Contractors...

Firewall is informed by XMC if the end-system is disconnected from the network, so firewall can close all opened sessions. Session can't be hijacked.

If firewall detects the Spyware or Virus or any kind of threat then XMC will be informed and XMC will perform action at the place where the end-system is connected. Example of such action is applying quarantine security policy profile.

### Extreme Policy vs. Firewall

Extreme Policy (One Policy) is applied on the PEP (Policy Enforcement Point) = as close to the end system as possible = usually first port / Access Point where the end system is connected.

Firewall rules are applied inline on the firewall. Firewall is usually placed between two security zones.

Firewall can block the traffic much deeper in the network while Policy is much closer to the edge.

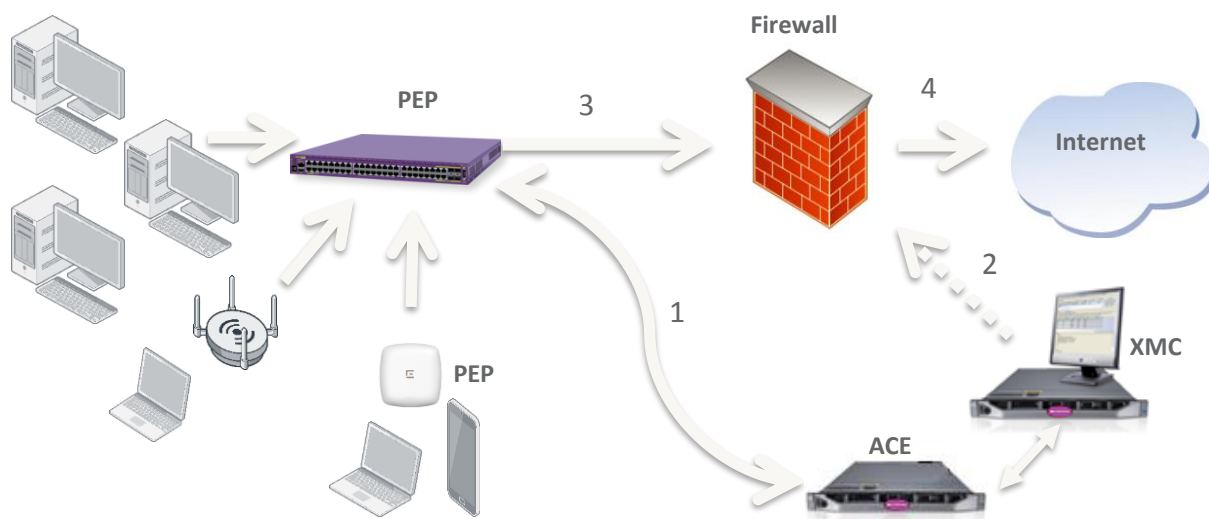
Extreme Policy can apply the QoS, VLAN, Filtering...

Firewall can apply QoS, ACLs, DPI (Deep Packet Inspection) = Antivirus, AntiMallware, Application analytics, firewall rules are statefull.

Policy is applied in ASIC hardware = performance of Tbps for acceptable price, with many ports.

Firewall is software (some do have hardware acceleration) = performance of Gbps, lower number of ports, higher price.

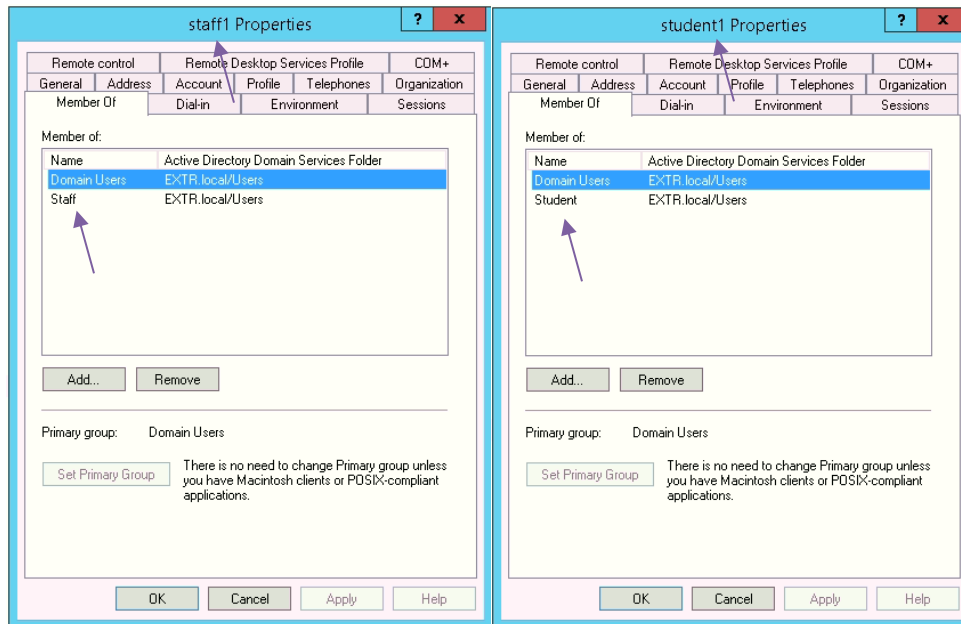
## How it works – XMC -> PaloAlto



0. End-system connects to the access switch / access point.
1. The radius communication reaches the Access Control Engine. ACE does process configuration rules and based on conditions the Access Control Profile is chosen. Access Control Profile does assign Security Policy Profile. The Radius Access Accept is sent to the access switch / access point. There can be Security Policy Profile in the Radius Access Accept.
2. When the address resolution is finished (the XMC knows the IP address of the end-system) the user-id mapping is sent to the firewall through the API.
3. Firewall does apply its configuration on the traffic from the end-system. Based on the information from the XMC the firewall knows the username for the source IP.
4. Traffic is inspected by the firewall with rules reflecting the Username.

## LDAP -> Extreme Control -> Policy -> XMC -> PaloAlto

User “staff1” is part of the “Staff” group in the AD, “student1” is part of “Student” group:



Users are authenticated, IP addresses are resolved, Policy is applied on PEP, security policy profile is assigned:

State	Last Seen	IP Address	MAC Address	MAC OUI Vendor	Host Name	Device Family	Device Type	User Name
✓	06/02/2018 22:23:48	192.168.10.127	28.6A.BA.EE.5F.4E	Apple	ipad-Zdenek	Apple iOS	iPhone/iPad/iPod/Watch/ATV	student1
✓	06/02/2018 22:22:52	192.168.10.205	64.20.0C.65.34.3C	Apple, Inc.	HelcaZuzka-iPad	Apple iOS	iPhone/iPad/iPod/Watch/ATV	Staff1
✓	06/02/2018 22:20:51	192.168.10.209	20.B3.99.D7.23.F2	Enterasys	AP2	Wireless Access Point	Extreme Identifi Wireless Access Point	
✓	29/07/2017 10:18:43	192.168.10.207	D8.84.66.32.27.31	Extreme Networks, I...	AP3	Wireless Access Point	Extreme Identifi Wireless Access Point	
✓	28/10/2016 22:03:30	192.168.13.180	00.01.E3.2D.6B.1A	Siemens AG	1000	Linux	Linux Siemens OpenStage 20/40/60/80	
✓	15/10/2016 12:25:50	192.168.10.170	00.40.8C.B4.31.E7	AXIS COMMUNICA...	axis-00408cb43...	Other	Enterasys HiPath Wireless Access Point 36...	
✓	05/10/2016 13:52:01	192.168.10.171	BC.92.6B.40.AA.51	Apple, Inc.	Zdenda-iPhone	Apple iOS	iPhone/iPad/iPod/ATV	Manson, Marilyn
✓	03/10/2016 13:34:10	192.168.10.3	00.26.B9.E3.33.69	Dell Inc.	ZPALA-WS	Windows	Windows Vista/ 7/ 2008	
✓	20/09/2016 17:22:58	10.0.1.243	7C.D1.C3.E4.07.1F	Apple, Inc.	iUrbans-MB-Air	Mac	OS X Lion/ Mountain Lion	
✓	20/09/2016 17:02:49	10.0.0.8	10.0B.A9.C2.A3.04	Intel Corporate	Queeq	Linux	Linux Ubuntu	
✓	20/09/2016 15:59:09	192.168.10.118	D4.C1.FC.8A.CA.43	Nokia Corporation		SymbianOS	Symbian OS	Jones, Marilyn
✓	20/09/2016 11:56:22	10.0.0.200	00.01.36.DD.CF.9B	CyberTAN Technolo...	android_5b11d...	Android	Nook	
✓	20/09/2016 10:59:35	10.0.1.206	28.EF.01.50.41.4F	Private	dhcp-10-0-1-206	Amazon Kindle	Amazon Kindle	
✓	06/09/2016 9:00:39	192.168.10.2	E0.94.67.07.D8.DC	Intel Corporate	nb-chalotaj	Windows	Windows 8	
✓	05/09/2016 13:08:00	192.168.10.110	40.2B.A1.BE.B2.BC	Sony Mobile Comm...		Other	Fluke OneTouch Series II 10/100	student1

Device Family	Device Type	User Name	Switch IP	Switch Nickname	Switch Port	Policy	Profile
Apple iOS	iPhone/iPad/Watch/ATV	student1	192.168.10.250	EWC1	AP2 (20-B3-99-D8-58-30).SingleSSID	Student	Student
Apple iOS	iPhone/iPad/iPod/Watch/ATV	Staff1	192.168.10.250	EWC1	AP2 (20-B3-99-D8-58-30).SingleSSID	Staff	Staff
Wireless Access Point	Extreme IdentifiFi Wireless Access Point		192.168.10.13	X440G2		AccessPoint	AccessPoint
Wireless Access Point	Extreme IdentifiFi Wireless Access Point		192.168.10.13	X440G2	AP (1.8)	AccessPoint	AccessPoint
Linux	Linux Siemens OpenStage 20/40/60/80		192.168.10.10	D2-Demokit	Phone (ge.1.5)	IPPhone	IPPhone
Other	Enterasys HiPath Wireless Access Point 36...		192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9).DemoNet-Guest	Unregistered	Unregistered
Apple iOS	iPhone/iPad/iPod/ATV	Manson, Marilyn	192.168.10.250	EWC1	AP5 (20-B3-99-A5-DE-60).SingleSSID	Guest Access	Guest Access
Windows	Windows Vista/ 7/ 2008		192.168.10.10	D2-Demokit	MACauth (ge.1.3)	Unregistered	Unregistered
Mac	OS X Lion/ Mountain Lion		192.168.10.250	EWC1	AP5 (00-1F-45-99-5F-B8).IT_konference	Unregistered	Unregistered
Linux	Linux Ubuntu		192.168.10.250	EWC1	AP3 (00-1F-45-99-5E-B3).IT_konference	Unregistered	Unregistered
SymbianOS	Symbian OS	Jones, Marilyn	192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9).DemoNet-Guest	Guest Access	Guest Access
Android	Nook		192.168.10.250	EWC1	AP3 (00-1F-45-99-5E-BB).IT_konference	Unregistered	Unregistered
Amazon Kindle	Amazon Kindle		192.168.10.250	EWC1	AP3 (00-1F-45-99-5E-BB).IT_konference	Unregistered	Unregistered
Windows	Windows 8		192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9).DemoNet-Guest	Unregistered	Unregistered
Other	Fluke OneTouch Series II 10/100	student1	192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9).DemoNet-Guest	Guest Access	Guest Access

Rules are using usernames in condition and rules apply AntiVirus & URL filtering & Anti-Spyware & ... specific for the Students, other settings are applied to Staff:

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
1 Student To StaffServer	none	interzone	Untrusted	any	Student1	any	Trusted	StaffServer	any	service-http	Drop	none	
2 Student SSH To StaffServer	none	interzone	Untrusted	any	Student1	any	Trusted	StaffServer	SSH	any	Drop	none	
3 Students Access	none	interzone	Untrusted	any	Student1	any	Trusted	any	any	application-d...	Allow	Antivirus Profiles: Students Antivirus	
4 Staff Access	none	interzone	Untrusted	any	Staff1	any	Trusted	any	any	application-d...	Allow	Antivirus Profiles: Students Antivirus	
5 MGMT access	none	interzone	Trusted	any	any	any	Trusted	any	any	any	Allow	none	
6 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
7 interzone-default	none	interzone	any	any	any	any	any	any	any	any	Deny	none	none

More complete picture of Firewall rules:

The screenshot shows the Palo Alto Networks GUI with the 'Policies' tab selected. A table lists three security policy rules. The 'Students Access' rule is highlighted, and its configuration window is open. The 'Profile Setting' section is highlighted with a purple box.

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address
1 Student To StaffServer	none	interzone	Untrusted	any	Student1 Student2	any	Trusted	StaffSe
2 Student SSH To StaffServer	none	interzone	Untrusted	any	Student1 Student2	any	Trusted	StaffSe
3 Students Access	none	interzone	Untrusted	any	Student1 Student2	any	Trusted	any

**Security Policy Rule Configuration:**

- Action Setting:** Action: Allow; Send ICMP Unreachable:
- Log Setting:** Log at Session Start: ; Log at Session End: ; Log Forwarding: None
- Profile Setting (highlighted):**
  - Profile Type: Profiles
  - Antivirus: Students Antivirus
  - Vulnerability Protection: Students Vulnerability
  - Anti-Spyware: Students-Spyware
  - URL Filtering: Students Filtering
  - File Blocking: strict file blocking
  - Data Filtering: None
  - WildFire Analysis: Students WildFire
- Other Settings:** Schedule: None; QoS Marking: None; Disable Server Response Inspection:

The screenshot shows the Palo Alto Networks GUI with the 'Policies' tab selected. A table lists four security policy rules. The 'Staff Access' rule is highlighted, and its configuration window is open. The 'Profile Setting' section is highlighted with a purple box.

Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address
1 Student To StaffServer	none	interzone	Untrusted	any	Student1 Student2	any	Trusted	StaffSe
2 Student SSH To StaffServer	none	interzone	Untrusted	any	Student1 Student2	any	Trusted	StaffSe
3 Students Access	none	interzone	Untrusted	any	Student1 Student2	any	Trusted	any
4 Staff Access	none	interzone	Untrusted	any	Staff1 Staff2	any	Trusted	any

**Security Policy Rule Configuration:**

- Action Setting:** Action: Allow; Send ICMP Unreachable:
- Log Setting:** Log at Session Start: ; Log at Session End: ; Log Forwarding: None
- Profile Setting (highlighted):**
  - Profile Type: Profiles
  - Antivirus: Staffs Antivirus
  - Vulnerability Protection: Staffs Vulnerability
  - Anti-Spyware: Staffs-Spyware
  - URL Filtering: Staffs Filtering
  - File Blocking: basic file blocking
  - Data Filtering: None
  - WildFire Analysis: Staffs WildFire
- Other Settings:** Schedule: None; QoS Marking: None; Disable Server Response Inspection:



## Online monitor of the rule usage:

The screenshot shows the Palo Alto Networks Monitor interface. The left sidebar contains navigation options like Logs, Traffic, Threat, URL Filtering, WildFire Submissions, Data Filtering, HIP Match, User-ID, Tunnel Inspection, Configuration, System, Alarms, Authentication, Unified, Packet Capture, App Scope, Session Browser, Botnet, PDF Reports, Manage PDF Summary, User Activity Report, SaaS Application Usage, Report Groups, Email Scheduler, Manage Custom Reports, and Reports.

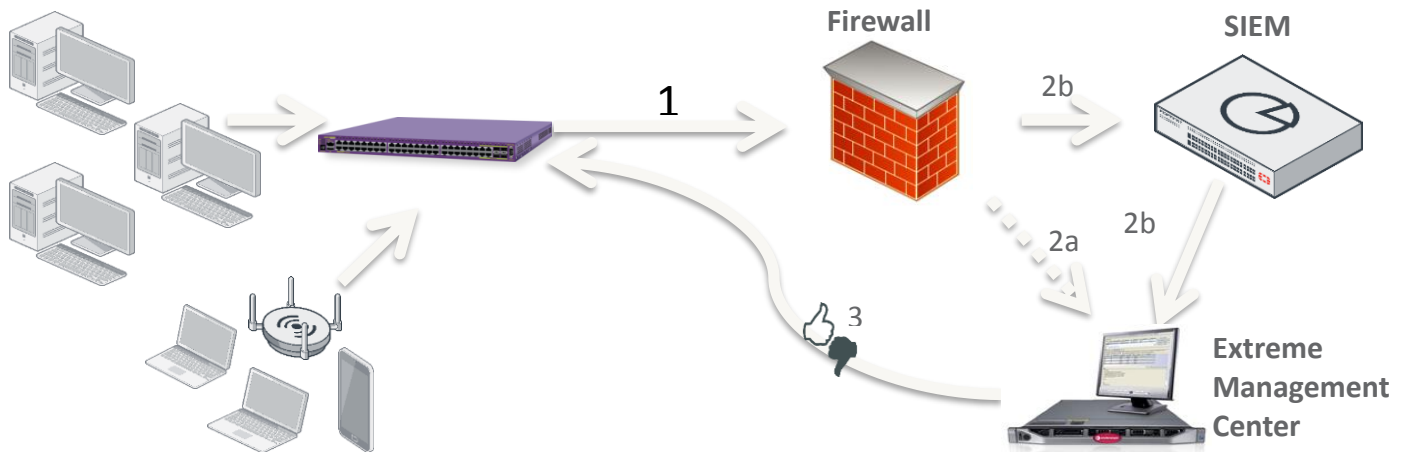
The main content area displays a table of rule usage with columns: Start Time, From Zone, To Zone, Source, Destination, From Port, To Port, Protocol, Application, and Rule. Two rows are highlighted with blue arrows pointing to the 'Rule' column: 'Staff Access' and 'Students Access'.

Below the table, a 'Detail' section provides further information for the selected rule, including Session ID, Timeout, Virtual System, Application, Protocol, Security Rule, URL Category, QoS Rule, QoS Class, Created By, To Host Session, Traverse Tunnel, Captive Portal, Session End Log, Session In Ager, and Session From HA.

This screenshot shows the Palo Alto Networks Monitor interface with a filter applied: '(destination eq 192.168.30.1)'. The table displays filtered rule usage entries with columns: Start Time, From Zone, To Zone, Source, Destination, From Port, To Port, Protocol, Application, Rule, Ingress I/F, and Egress I/F.

The table shows several entries for 'web-browsing' and 'ssh' applications, all associated with the 'Staff Access' rule. The 'Ingress I/F' and 'Egress I/F' columns show traffic passing through 'ethernet1/1' and 'ethernet1/2' interfaces.

## How Distributed IPS (DIPS) works – PaloAlto -> XMC



1. User traffic is analyzed by NG firewall. (Firewall, AV, AntiSpyware, URL filtering etc.)
2. Security incidents are reported to Extreme Management Center (and SIEM)
3. Extreme Management Center can apply dynamic reaction based on attributes of that security incident.  
E. g.: Quarantine the user at the network point of presence (switch, wireless AP, VPN)

## DIPS: PaloAlto -> XMC

There is user “Student1” logged in to the network. The security policy profile “Student” is applied:

Device Family	Device Type	User Name	Switch IP	Switch Nickname	Switch Port	Policy	Profile
Apple iOS	iPhone/iPad/iPod/Watch/ATV	student1	192.168.10.250	EWC1	AP2 (20-B3-99-D8-58-30):SingleSSID	Student	Student
Apple iOS	iPhone/iPad/iPod/Watch/ATV	Staff1	192.168.10.250	EWC1	AP2 (20-B3-99-D8-58-30):SingleSSID	Staff	Staff
Wireless Access Point	Extreme Identifi Wireless Access Point		192.168.10.13	X440G2	AP (1.8)	AccessPoint	AccessPoint
Linux	Linux Siemens OpenStage 20/40/60/80		192.168.10.10	D2-Demokit	Phone (ge.1.5)	IPPhone	IPPhone
Other	Enterasys HiPath Wireless Access Point 36...		192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9):DemoNet-Guest	Unregistered	Unregistered
Apple iOS	iPhone/iPad/iPod/ATV	Manson, Marilyn	192.168.10.250	EWC1	AP5 (20-B3-99-A5-DE-60):SingleSSID	Guest Access	Guest Access
Windows	Windows Vista/ 7/ 2008		192.168.10.10	D2-Demokit	MACauth (ge.1.3)	Unregistered	Unregistered
Mac	OS X Lion/ Mountain Lion		192.168.10.250	EWC1	AP5 (00-1F-45-99-5F-B8):IT_konference	Unregistered	Unregistered
Linux	Linux Ubuntu		192.168.10.250	EWC1	AP3 (00-1F-45-99-5E-B3):IT_konference	Unregistered	Unregistered
SymbianOS	Symbian OS	Jones, Marilyn	192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9):DemoNet-Guest	Guest Access	Guest Access
Android	Nook		192.168.10.250	EWC1	AP3 (00-1F-45-99-5E-BB):IT_konference	Unregistered	Unregistered
Amazon Kindle	Amazon Kindle		192.168.10.250	EWC1	AP3 (00-1F-45-99-5E-BB):IT_konference	Unregistered	Unregistered
Windows	Windows 8		192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9):DemoNet-Guest	Unregistered	Unregistered
Other	Fluke OneTouch Series II 10/100	student1	192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9):DemoNet-Guest	Guest Access	Guest Access

If “Student1” or “Student2” does SSH to the Staff server then the XMC is informed:

Name	Tags	Type	Zone	Address	User	Profile	Zone	Address	Application	Service	Action	Profile	Options
1 Student To StaffServer	none	interzone	Untrusted	any	Student1	any	Trusted	StaffServer	any	service-http	Drop	none	Quarantine
2 Student SSH to StaffServer	none	interzone	Untrusted	any	Student1	any	Trusted	StaffServer	SSH	any	Drop	none	Quarantine
3 Students Access	none	interzone	Untrusted	any	Student2	any	Trusted	any	any	application-d...	Allow	none	AccessP...
4 Staff Access	none	interzone	Untrusted	any	Staff1	any	Trusted	any	any	application-d...	Allow	none	AccessP...
5 MGMT access	none	interzone	Trusted	any	Staff2	any	Trusted	any	any	any	Allow	none	AccessP...
6 intrazone-default	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow	none	none
7 intrazone-default	none	intrazone	any	any	any	any	any	any	any	any	Deny	none	none

I can ping the student device. When I open SSH session from Student device to the staffserver I am quarantined:

State	Last Seen	IP Address	MAC Address	MAC OUI	Vendor	Host Name	Device Family	Device Type	User Name	Switch IP	Switch Nickname	Switch Port	Policy
Green	07/02/2018 0:03:18	192.168.10.127	28.6A.BA.EE.5F.4E	Apple	Apple	ipad-Zdenek	Apple iOS	iPhone/iPad/iPod/Watch/TV	student1	192.168.10.250	EWC1	AP2 (20-B3-99-D8-58-30) SingleSSID	Quarantine DIPS
Green	07/02/2018 0:03:07	192.168.10.205	64.20.0C.65.34.3C	Apple, Inc.	Apple	HelcaZucka-iPad	Apple iOS	iPhone/iPad/iPod/Watch/TV	Staff1	192.168.10.250	EWC1	AP2 (20-B3-99-D8-58-30) SingleSSID	Staff
Green	06/02/2018 22:28:51	192.168.10.209	28.83.99.D7.23.F2	Enterasys	AP2	Wireless Access Point	Extreme IdentIFI Wireless Access Point			192.168.10.13	X44802		AccessP...
Green	29/07/2017 10:18:43	192.168.10.207	D8.84.66.32.27.31	Extreme Networks, I.	AP3	Wireless Access Point	Extreme IdentIFI Wireless Access Point			192.168.10.13	X44802	AP (1.8)	AccessP...
Green	28/10/2016 22:03:30	192.168.13.180	00.01.E3.2D.68.1A	Siemens AG	1000	Linux	Linux Siemens OpenStage 20-40/60/80			192.168.10.10	D2-Demokit	Phone (ge.1.5)	IPPhone
Green	15/10/2016 12:25:50	192.168.10.170	08.40.8C.B4.31.E7	AXIS COMMUNICA...	axis-00408cb43...	Other	Enterasys HiPath Wireless Access Point ...			192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9) DemoNet-Guest	Unregistered
Green	05/10/2016 13:52:01	192.168.10.171	BC.92.6B.4D.AA.51	Apple, Inc.	Zdena-iPhone	Apple iOS	iPhone/iPad/iPod/ATV	Manson, Mar...		192.168.10.250	EWC1	AP5 (20-B3-99-A5-DE-60) SingleSSID	Guest Access
Green	03/10/2016 13:34:10	192.168.10.3	08.26.B9.E3.33.69	Dell Inc.	ZPALA-WS	Windows	Windows Vista/ 7/ 2008			192.168.10.10	D2-Demokit	MACauth (ge.1.3)	Unregistered
Green	20/09/2016 17:22:58	10.0.1.243	7C.D1.C3.E4.07.1F	Apple, Inc.	iUrbans-MB-Air	Mac	OS X Lion/ Mountain Lion			192.168.10.250	EWC1	AP5 (00-1F-45-99-4F-B8) IT_konference	Unregistered
Green	20/09/2016 17:02:49	10.0.0.8	10.0B.A9.C2.A3.04	Intel Corporate	Quesq	Linux	Linux Ubuntu			192.168.10.250	EWC1	AP3 (00-1F-45-99-4E-B3) IT_konference	Unregistered
Green	20/09/2016 15:59:09	192.168.10.118	D4.C1.FC.8A.CA.43	Nokia Corporation		SymbianOS	Symbian OS	Jones, Marilyn		192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9) DemoNet-Guest	Guest Access
Green	20/09/2016 11:56:22	10.0.0.200	00.01.36.D0.CF.9B	CyberTAN Technolo...	android_Sb11d...	Android	Noak			192.168.10.250	EWC1	AP3 (00-1F-45-99-4E-BB) IT_konference	Unregistered
Green	20/09/2016 10:59:35	10.0.1.206	28.EF.01.50.41.4F	Private	dhcp-10.0.1-206	Amazon Kindle	Amazon Kindle			192.168.10.250	EWC1	AP3 (00-1F-45-99-4E-BB) IT_konference	Unregistered
Green	06/09/2016 9:00:39	192.168.10.2	E0.94.67.07.D8.DC	Intel Corporate	nb-chalotaj	Windows	Windows 8			192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9) DemoNet-Guest	Unregistered
Green	05/09/2016 13:08:00	192.168.10.110	40.2B.A1.BE.B2.BC	Sony Mobile Comm...		Other	Fluke OneTouch Series II 10/100	student1		192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9) DemoNet-Guest	Guest Access
Green	05/09/2016 10:49:51	192.168.10.116	7C.61.93.3E.D7.A2	HTC Corporation	Android_35681...	Android	Android	Smith, John		192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9) DemoNet-Guest	Unregistered
Green	04/09/2016 13:48:47	192.168.10.117	00.1D.FE.D2.DA.EC	Palm, Inc.		Linux	Linux Debian 3.1			192.168.10.250	EWC1	AP1 (00-1F-45-5A-EC-F9) DemoNet-Guest	Unregistered
Green	30/08/2016 13:44:45	192.168.10.122	F0.7B.CB.20.C0.59	Hon Hai Precision I...	Skorpik	Windows	Windows 7 Ultimate (Windows 7 SP1)	Williams, Ivan		192.168.10.250	EWC1	AP3620 (00-1F-45-5A-EC-F1) DemoNet...	Quarantine_NAC
Green	10/05/2016 12:44:29	192.168.10.132	88.70.8A.44.0F.9C	Murata Manufaktur...	android-hh1Q9	Android	Galaxy Nexus	Williams, Ivan		192.168.10.250	FWC1	AP/W20 (00-1F-45-5A-F-C-F) DemoNet...	Android

St...	Time Stamp	Access Contr...	Profile	IP Address	MAC Address	User Name	Host Name	Device Family	Device Type	State Description	Extended S...	Reason
Green	07/02/2018 0:03:18	192.168.30.35	Quarantine DIPS Profile		28.6A.BA.EE.5F.4E	student1	ipad-Zdenek	Apple iOS	iPhone/iPad/iPod/Watch/...	Resolving IP...	Rule: "Blacklist"	
Green	07/02/2018 0:02:52	192.168.30.35	Student	192.168.10.127	28.6A.BA.EE.5F.4E	student1	ipad-Zdenek	Apple iOS	iPhone/iPad/iPod/Watch/...	This end-system has moved to ...	No Error	Rule: "Student on CaptivePor"
Green	07/02/2018 0:02:51	192.168.30.35	Student	192.168.10.127	28.6A.BA.EE.5F.4E	student1	ipad-Zdenek	Apple iOS	iPhone/iPad/iPod/Watch/...	This end-system has moved to ...	No Error	Rule: "Student on CaptivePor"
Green	07/02/2018 0:02:48	192.168.30.35	Student		28.6A.BA.EE.5F.4E	student1	ipad-Zdenek	Apple iOS	iPhone/iPad/iPod/Watch/...	Resolving IP...	Rule: "Student on CaptivePor"	
Green	06/02/2018 23:54:43	192.168.30.35	Student	192.168.10.127	28.6A.BA.EE.5F.4E	student1	ipad-Zdenek	Apple iOS	iPhone/iPad/iPod/Watch/...	The session is no longer active ...	No Error	Rule: "Student on CaptivePor"
Green	06/02/2018 23:46:25	192.168.30.35	Student	192.168.10.127	28.6A.BA.EE.5F.4E	student1	ipad-Zdenek	Apple iOS	iPhone/iPad/iPod/Watch/...	This end-system has moved to ...	No Error	Rule: "Student on CaptivePor"

The PaloAlto rule name is part of the reason description:

The screenshot shows the Palo Alto Networks management console interface. The top navigation bar includes 'Dashboard', 'Policy', 'Access Control', 'End-Systems', 'Reports', and 'End-System Details - ipad-Zdenek'. Below this, there are tabs for 'Access Profile', 'End-System', 'End-System Events', and 'Health Results'. A secondary navigation bar contains icons for 'Add To Group', 'Force Reauthentication', 'Force Reauthentication and Scan', 'Lock MAC', and 'Edit Registration'. The main content area is titled 'End-System Details' and contains the following information:

- End-System: 28:6A:BA:EE:5F:4E, 192.168.10.127, ipad-Zdenek
- User Name: student1
- Activity: Last seen 02/07/2018 12:03:18 AM, First seen 02/06/2018 10:21:15 PM
- Device Information: Apple iOS (iPhone/iPad/iPod/Watch/ATV)
- Location: 192.168.10.250/AP2 (20-B3-99-D8-58-30):SingleSSID, Demokit-1st floor, Default, 192.168.30.35
- Authentication Sessions
- Registration:
- Miscellaneous: Not NAP Capable
- Custom Information: None
- Groups

The 'Groups' section contains a table with the following data:

	Name	Type	Group Description	Entry Description
	Blacklist	MAC	End-Systems denied ...	Student SSH To StaffServer

A blue arrow points to the 'Entry Description' field of the 'Blacklist' group, which contains the text 'Student SSH To StaffServer'.

## Configuration options XMC

### SNMP configuration (not necessary for User-ID mapping):

**Edit SNMP Credential: v3s-cred**

Credential Name: v3s-cred

SNMP Version: SNMPv3

User Name: snmpuser

Authentication Type: SHA

Authentication Password: .....

Privacy Type: AES

Privacy Password: .....

**Edit Profile: snmp\_v3s\_profile**

Profile Name: snmp\_v3s\_profile

SNMP Version: SNMPv3

Read: v3s-cred Read Security: AuthPriv

Write: v3s-cred Write Security: AuthPriv

Max Access: v3s-cred Max Security: AuthPriv

CLI Credential: PaloAlto

PaloAlto does require **Authentication Type: SHA**

PaloAlto does require **Privacy Type: AES**

Vendor Profile configuration (beta feature in XMC version 8.0 and 8.1.1) (not necessary for User-ID mapping):

Scheduler Scripting Profiles Users Server Information Certificates Options Backup/Restore Diagnostics **Vendor Profiles**

Vendor Profiles ↑

Vendors

- Palo Alto
  - Palo Alto
    - Palo Alto
      - PA-2020
      - PA-3020
      - PA-500
      - PA-VM-100

**Edit Vendor Profile: PA-VM-100**

Add... Edit... Delete...

Name	Value ↑
Subfamily	
Company OID	1.3.6.1.4.1.25461
OID	1.3.6.1.4.1.25461.2.3.29
Element Type	Device
Device Type	PA-VM-100
OID Name	PA-VM-100
Image	PA-VM-picture.png
Family	Palo Alto
Webview	https://%IP.443

OID is SysObjectID = unique identifier for the device type. Different products does have different SysObjectID. You can determine the SysObjectID by mibtools or by XMC OneView -> Network -> right click on the device -> Device -> Configure Device -> Vendor Profile Definition

## Connect configuration:

Name	Enabled	ID	username	password	server	uidEnabled	uidNac	uidServer	uidPort	uidDomain	uidVsys	uidMultiUserTimer	uidStripEmailDomain	uidStripDomainName	uidStripDomainUse...
1	✓	1	apuser	*****	192.168.30.56	✓			5006		vsys1	5	✗	✗	

**ID** = you can have more PaloAlto firewalls

**Username** = username the API call will use. The username must match with the PaloAlto config.

**Password** = password the API call will use. The password must match with the PaloAlto config.

**Server** = This should be the management IP of the Palo Alto firewall.

**uidEnabled** = if not enabled the User-ID mapping will not work.

**uidPort** = default port for the agent = 5006

Name	Description	Value
Poll interval in seconds	The time the module will wait during each run	60
Module loglevel	The module loglevel setting (DEBUG, INFO, WARN, ERROR...)	ERROR
Module enabled	En-/Disables the module	✓
Update local data from remote ser...	If this is set to true, data from the remote service will be used...	✓
Enable Data Persistence	Enabling this option will force the module to store endsystem...	✓

Name	Description	Value
Maximum Number of calls/second	The maximum number of user-ID messages to Palo Alto per ...	5
Maximum Number of processing t...	Maximum Number of processing threads	8
Enable reverse DNS lookup	Enable reverse DNS lookup, default behavior is true	✓
Webservice Timeout	Timeout, in seconds, for Palo Alto web service call	60
Reuse HTTP connection	Reuse HTTP connection to limit connections to Palo Alto	✗
Use global endsystem groups	Enable this to import EndSystem Groups defined by other m...	✓

**Poll interval in seconds** = how often will PaloAlto module wait between cycles. This should stay at the default value of 60.

**Module loglevel** = verbosity of the PaloAlto module. Log file is standard server.log

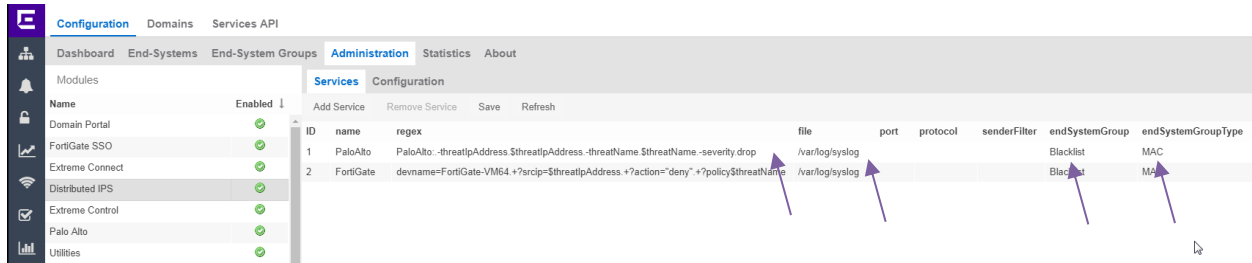
**Module enabled** = if you want to use this module or not.

**Update local data from remote service** = This should be left as true.

**Enable Data Persistence** = This should remain as true.

**Use global endsystem groups** = This should be left as true.

## DIPS configuration:



**ID** = you can have more rules

**Name** = name of the rule for humans

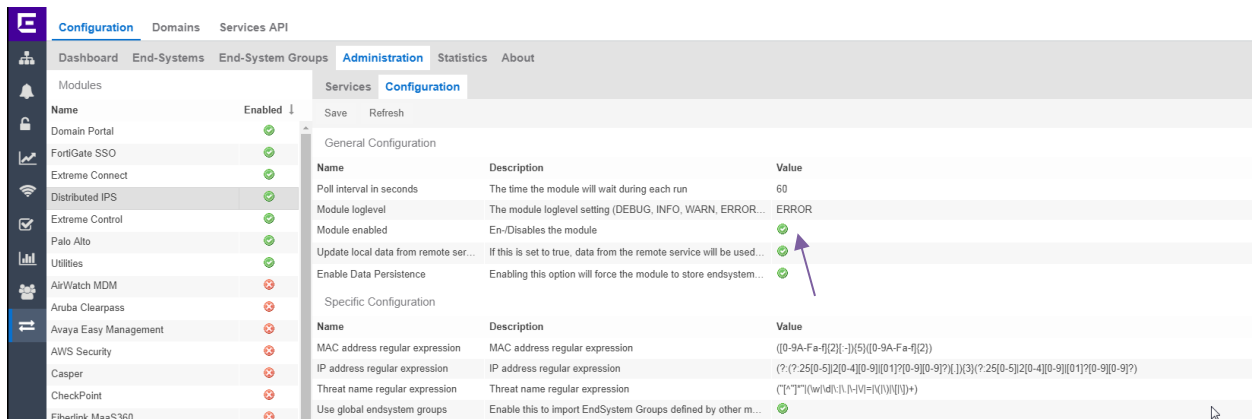
**Regex** = definition of what DIPS module search:

PaloAlto:.-threatIpAddress.\$threatIpAddress.-threatName.\$threatName.-severity.drop

**File** = we use syslog in this case

**endSystemGroup** = what group will the end-system be assigned

**endSystemGroupType** = the end-system group can be MAC or IP based...



Parameters can be adjusted from the **Configuration** subtab of the Distributed IPS module.

Most importantly, the **Module Enabled** value must be changed to **True**. Once the **Save** option is selected, the configuration is complete.

# Configuration options PaloAlto

If you want changes to take effect, do not forget to commit:

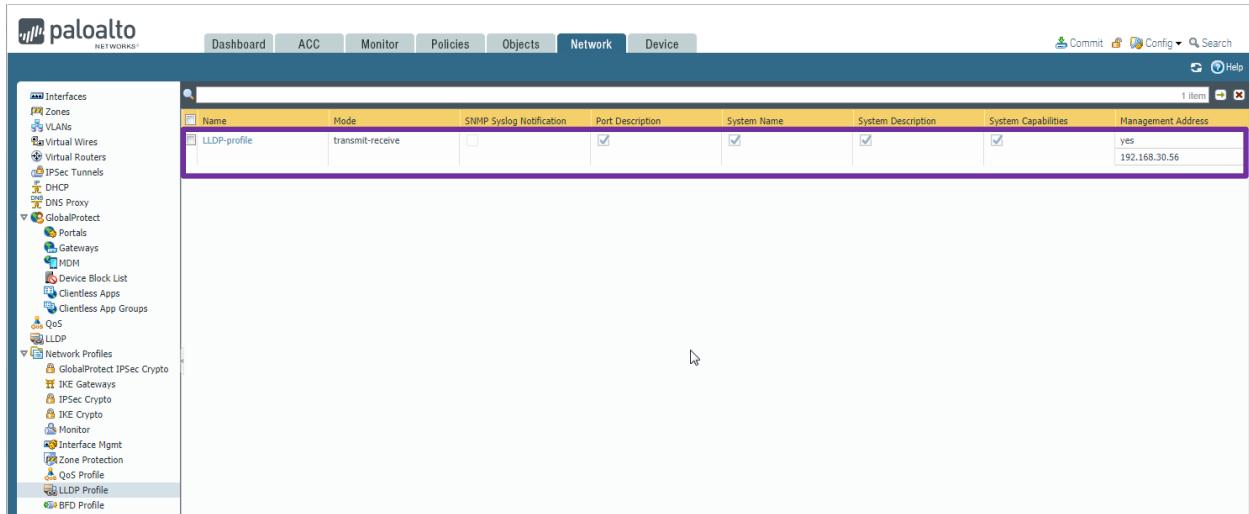
The screenshot shows the Palo Alto Networks configuration interface. At the top, there is a navigation bar with tabs for Dashboard, ACC, Monitor, Policies, Objects, Network, and Device. A 'Commit' button is visible in the top right corner. Below the navigation bar, the 'Device' tab is selected, and the 'Configuration Management' section is active. A dialog box titled 'SNMP Setup' is open, showing configuration options for a device named 'Demokit'. The dialog includes fields for Physical Location, Contact, and Version (V2c or V3). A table lists the configured users for SNMP traps.

Name	View	Auth Password	Priv Password
all	root: 1: include: undefined		
snmpuser	all	*****	*****

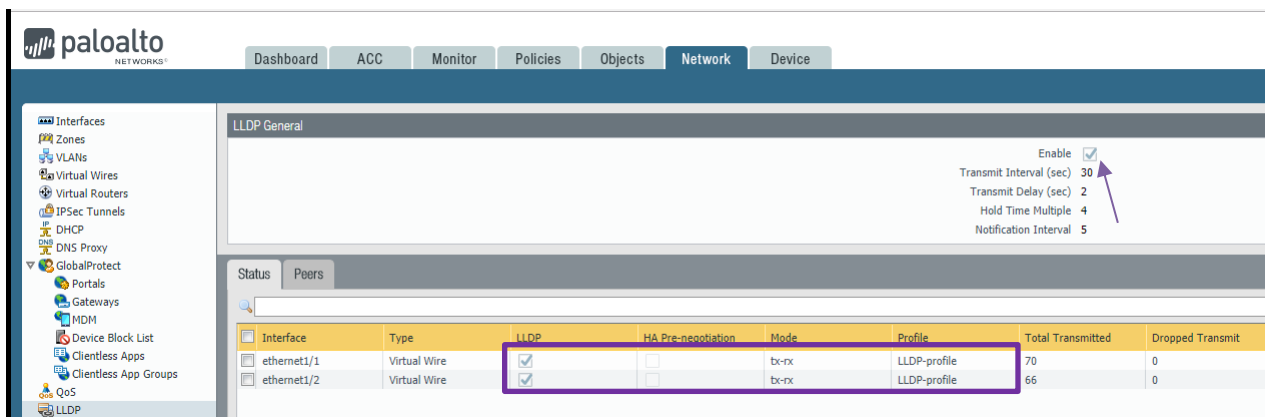
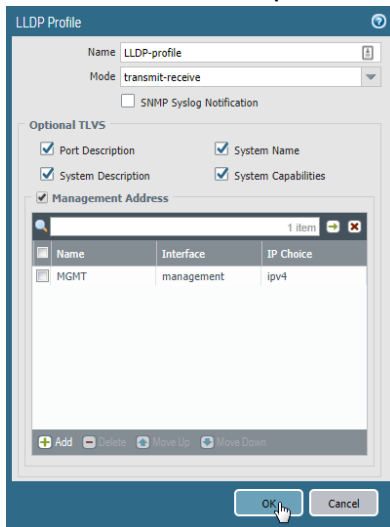
SNMP configuration (not necessary for User-ID mapping):



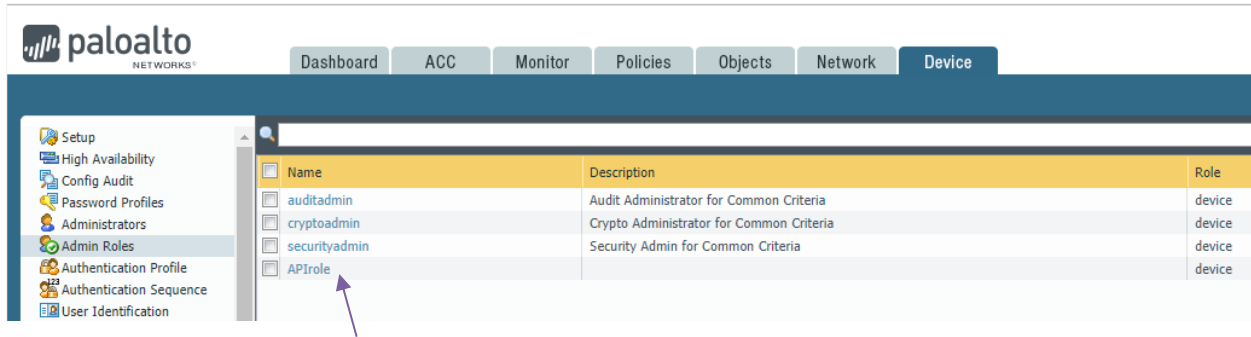
## LLDP configuration (not necessary for User-ID mapping):



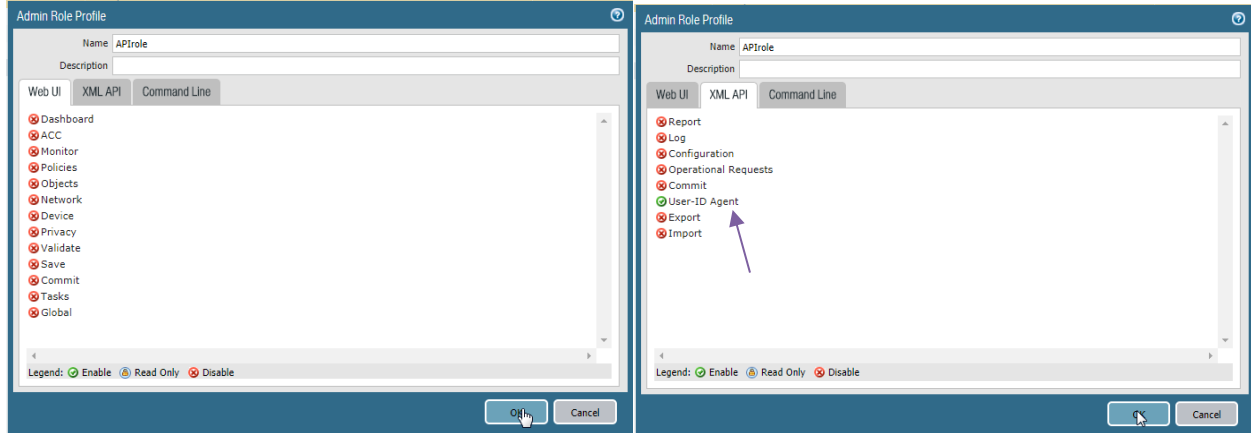
The IP in the LLDP profile should be the IP of the PaloAlto interface used for snmp.



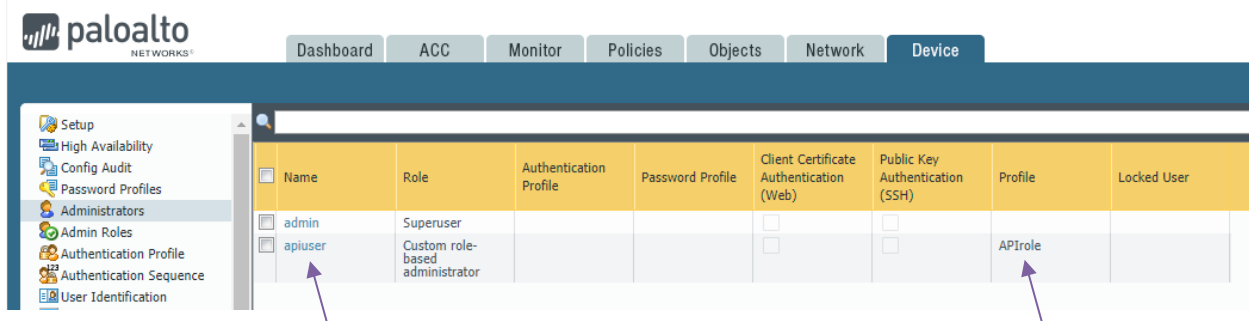
## API role (for User-ID integration):



## The role with authorization to call User-ID integration

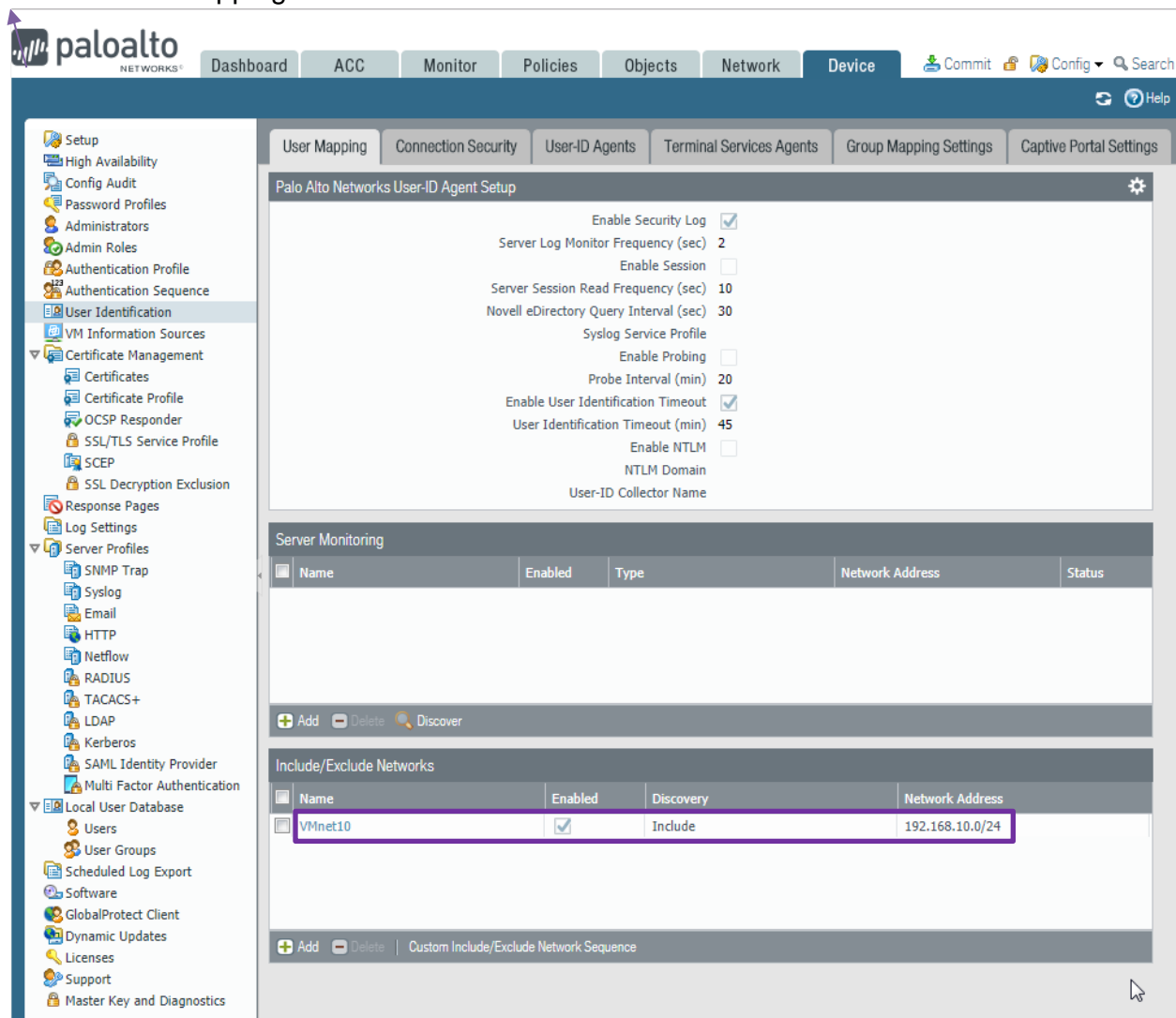


## API user (for User-ID integration):



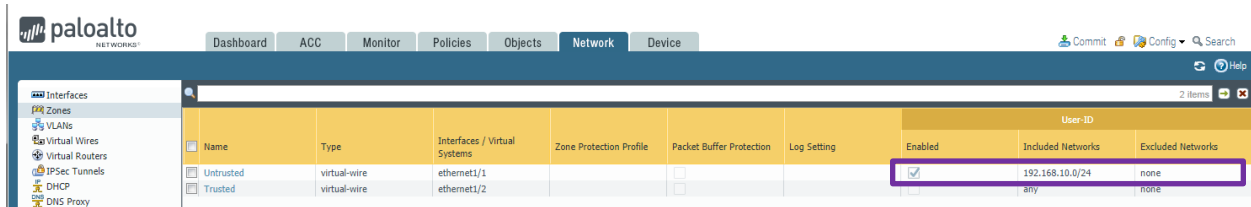
Username and password what XMC will use to update the User-ID mapping in the PaloAlto firewall.

## Enable User Mapping:



Include the IP subnet to the networks where User-ID mapping will be used.

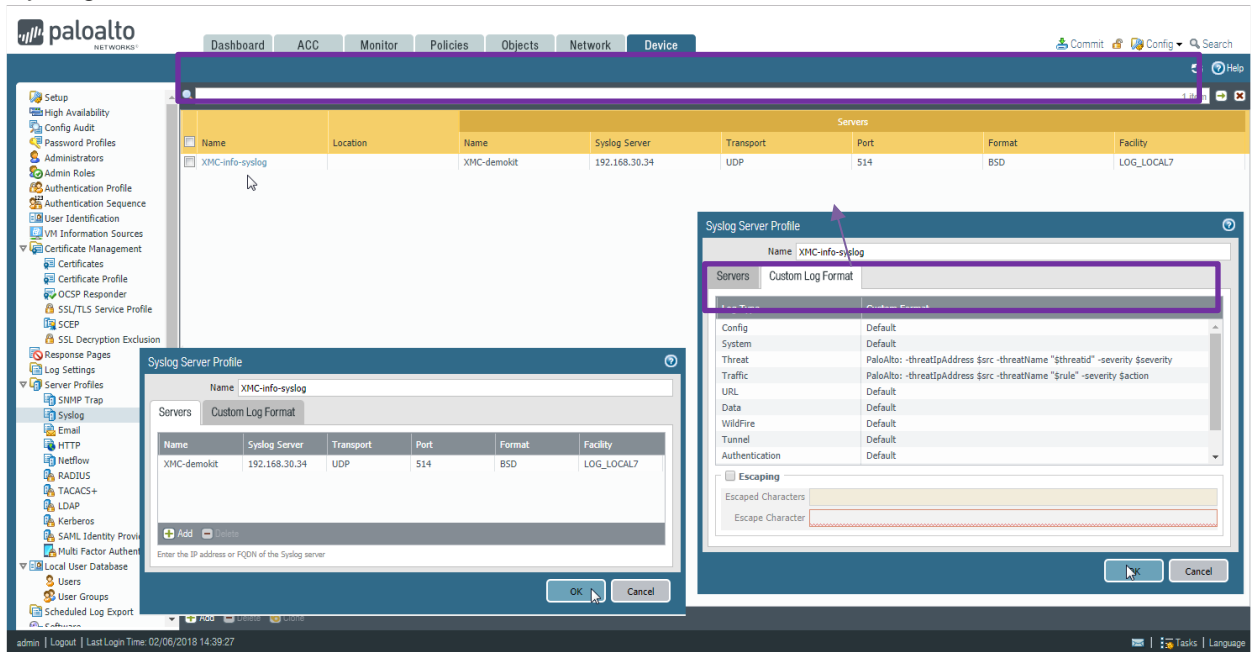
## Include & enable User-ID in the Zones menu:



Zone must have User-ID enabled and assigned subnet.

### DIPS configuration:

Syslog format and destination:



Custom format for the threat: **PaloAlto: -threatIpAddress \$src -threatName "\$threatid" - severity \$severity**

Custom format for the traffic: **PaloAlto: -threatIpAddress \$src -threatName "\$rule" - severity \$action**

### Logging Profile definition:

The screenshot shows the Palo Alto Networks GUI. On the left is a navigation tree with categories like Addresses, Applications, Services, Security Profiles, and Log Forwarding. The main area displays a table of logging profiles:

Name	Location	Description	Log Type	Filter	Panorama	SNMP	Email	Syslog
LoggingProfile			traffic	All Logs	<input type="checkbox"/>			XMC-info-syslog
			threat	All Logs	<input type="checkbox"/>			XMC-info-syslog

A modal window titled 'Log Forwarding Profile' is open, showing the configuration for the 'LoggingProfile'. It includes a table with 2 items:

Name	Log Type	Filter	Forward Method	Built-in Actions
Traffic-To-XMC-Syslog	traffic	All Logs	SysLog • XMC-info-syslog	
Threat-To-XMC-Syslog	threat	All Logs	SysLog • XMC-info-syslog	

Log forwarding profiles. One for traffic, one for threat. Each profile will use already defined syslog destination and format.

The image shows two side-by-side screenshots of the 'Log Forwarding Profile Match List' dialog boxes. The left dialog is for the 'Threat-To-XMC-Syslog' profile, and the right is for the 'Traffic-To-XMC-Syslog' profile. Both dialogs show the following configuration:

- Name: Threat-To-XMC-Syslog (left) / Traffic-To-XMC-Syslog (right)
- Description: (empty)
- Log Type: threat (left) / traffic (right)
- Filter: All Logs
- Forward Method: Syslog (selected), with 'XMC-info-syslog' listed as the destination.
- Built-in Actions: (empty)

## Terms & Condition of Use

---

Extreme Networks, Inc. reserves all rights to its materials and the content of the materials. No material provided by Extreme Networks, Inc. to a Partner (or Customer, etc.) may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, or incorporated into any other published work, except for internal use by the Partner and except as may be expressly permitted in writing by Extreme Networks, Inc.

This document and the information contained herein are intended solely for informational use. Extreme Networks, Inc. makes no representations or warranties of any kind, whether expressed or implied, with respect to this information and assumes no responsibility for its accuracy or completeness. Extreme Networks, Inc. hereby disclaims all liability and warranty for any information contained herein and all the material and information herein exists to be used only on an “as is” basis. More specific information may be available on request. By your review and/or use of the information contained herein, you expressly release Extreme from any and all liability related in any way to this information. A copy of the text of this section is an uncontrolled copy, and may lack important information or contain factual errors. All information herein is Copyright ©Extreme Networks, Inc. All rights reserved. All information contain in this document is subject to change without notice.

For additional information refer to: <http://www.extremenetworks.com/company/legal/terms/>

## Revision History

Date	Revision	Changes Made	Author
10/21/15	0.0	Initial Draft	J. Smart
02/07/18	0.9	Structure & Content based on PaloAlto version 8.0.5 and XMC version 8.1.1.41	Z. Pala
02/07/18	0.9.5	Added arrows, formatting, extended the Connect descriptions	Z. Pala